

Appl. No. 09/692,709
Amdt. Dated July 14, 2004
Reply to Office action of April 15, 2004
Attorney Docket No. P12266/45687-00038
EUS/JIP/04-6160

REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicants has amended Claims 1, 6, 17; Claim 2 has been cancelled. Applicants respectfully submit no new matter has been added. Accordingly, Claims 1, and 3-23 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Examiner Objections – Abstract

The Examiner objected to the Abstract because of certain informalities. The Applicants thank the Examiner for his careful review of the specification. In response, the Applicants have modified the Abstract as suggested by the Examiner. The Examiner's favorable reconsideration of the amended Abstract is respectfully requested.

4.) Examiner Objections - Claims

The Examiner objected to Claims 2 and 6-16 because of certain informalities. The Applicants have amended claim 2 as suggested by the Examiner and incorporated the subject matter recited thereto into Independent Claim 1. Accordingly, dependent Claim 2 has been cancelled without prejudice. Likewise, dependent Claims 6-16 have been amended to now depend, directly or indirectly, on independent Claim 1. A favorable reconsideration is respectfully requested.

5.) Claim Rejections – 35 U.S.C. § 102(e)

The Examiner rejected claims 1, 3-6, 17 and 18 under 35 U.S.C. § 102(e) as being anticipated by Chadwick. Applicants respectfully traverse the Examiner's rejection and have amended independent Claims 1 and 17 to more clearly and distinctly claim the subject matter which the Applicants believe as their invention. More specifically, the subject matter previous claimed in dependent Claim 2 has now been incorporated into independent Claim 1. A similar limitation has been added to Independent Claim 17.

Appl. No. 09/692,709
Amdt. Dated July 14, 2004
Reply to Office action of April 15, 2004
Attorney Docket No. P12288/45887-00036
EUS/JIP/04-6180

The present invention discloses and claims a system for establishing security in an ad hoc network. Unlike more established infrastructure or communication networks, the disclosed and claimed ad-hoc network lacks fixed infrastructure or communication networks. Such temporarily established communication networks serve special purposes, including military operations, rescue and recovery operation or remote construction sites, by using and interconnecting mobile phones, laptops, or other devices or communication members to establish an ad-hoc network. Unlike other conventional systems requiring separate "certificate solutions", in accordance with the teachings of the present invention, the ad-hoc communication network as claimed herein requires no separate certification authority (CA, as further disclosed on page 3-4 of the present application). However, even without the help of the certification authority, the desired security system is provided by allowing two or more nodes of the ad-hoc communication network to form a "trust group" using their public keys. After forming such a trust group, information received from another member of the trust group is "certified" and trusted by other members of the group.

In the event a particular non-trusted node (candidate node) desires to join the trust group, rather than relying on a centralized "certification authority" to allow the candidate node to be validated and to join the trust group, a particular node within the trust group having an existing trust relationship with the candidate node is first identified. The identified trusted node then "distributes" the trust relationship between all members of the trust group and the candidate node by distributing the public key associated with the candidate node to the trust group members. In other words, the remaining members of the trust group rely on the individual trust relationship previously established between the identified member and the candidate member to allow the candidate node to join the trust group and to share its public key information.

Applicants respectfully submit that independent Claim 1, as amended, is reproduced below for the Examiner's review:

1. A method for establishing security in an ad hoc communication network, the ad hoc communication network comprising a set of communication nodes, at least two nodes of the set of communication nodes having a mutual trust relation and

Appl. No. 09/692,709
Amtd. Dated July 14, 2004
Reply to Office action of April 15, 2004
Attorney Docket No. P12286/45687-00036
EUS/J/P/04-6160

comprising a trust group, the trust relations being created with public keys, and at least one additional node, the at least one additional node being a candidate node for joining the trust group within the ad hoc communication network, the nodes having authority to delegate trust to nodes of the set of communication nodes within the trust group, the method comprising the steps of:

receiving a request from the candidate node to join the trust group within said ad hoc communication network wherein said ad hoc communication network does not include a separate certificate authority;

identifying a node of the set of communication nodes within the trust group having a trust relation with the candidate node, the node having the trust relation with the candidate node being an X-node; and

distributing trust relations between all members in the trust group and the candidate node by means of the X-node distributing the public key associated with said candidate node to said all members of the trust group. (emphasis added).

Applicants respectfully submit that the Chadwick fails to anticipate or render obvious each and every element as currently recited by independent Claims 1 and 17. As a matter of facts, the Chadwick reference discloses using multiple central authorities (CAs) to establish the disclosed security system (Figs 3 and 4 of Chadwick on page 22). In Chadwick, each user has knowledge of the CA nodes that the user trusts. Accordingly, each user stores the public key of the trusted CA nodes in its personal security environment (PSE). This PSE further contains public keys and names of the users he/she trusts (Chadwick, Page 19, left column, the third paragraph). When the validation software is checking the validity of a certificate received from a certain user, it checks whether the policy id issued by the CA in the certificate is the same as the policy id in the user's PSE. In this way, the validation software enforces the trust configured into the Chadwick user's PSE.

However, in order for the Chadwick validation system to work, a separate certification authority (CA) has to issue a certificate and publish its security policies. Using such certificates and security policy, each user then updates its PSE and determines which users and associated information can be trusted.

Appl. No. 09/692,709
Amdt. Dated July 14, 2004
Reply to Office action of April 15, 2004
Attorney Docket No. P12266/45887-00036
EUS/J/P/04-6160

Accordingly, Chadwick actually teaches away from the present invention by requiring a separate certification authority (CA). Moreover, the recited trust group within an ad-hoc network is simply not disclosed or taught by Chadwick. Also, the step of identifying a particular node within the trust group having a trust relationship with a candidate node requesting admission to the trust group is further not disclosed or taught by Chadwick. Lastly, the step of the identified trusted node distributing trust relationships between all members of the trust group and the candidate node by distributing the public key associated with the candidate node to the remaining members of the trust group is also neither disclosed nor discussed by Chadwick. Furthermore, none of the portions of Chadwick cited by the Examiner (Pages 18, 20 and 22) anticipate or render obvious the above-mentioned steps. All those portions of Chadwick actually disclose using the CA to validate and to certify a particular user.

As a result, Independent Claims 1 and 17 are not anticipated or rendered obvious by Chadwick independently or in combination with Morris and a Notice of Allowance for the pending independent claims are earnestly requested.

6.) Claim Rejections – 35 U.S.C. § 103 (a)

The Examiner rejected claims 7-16 and 19-23 under 35 U.S.C. § 103(a) as being unpatentable over Chadwick in view of Morris et al (US 6,691,173). These dependent Claims depend from now allowable independent Claims 1 and 17 and recite further limitations in combination with the novel elements thereof. Therefore, the allowance of all of the pending claims is respectfully requested

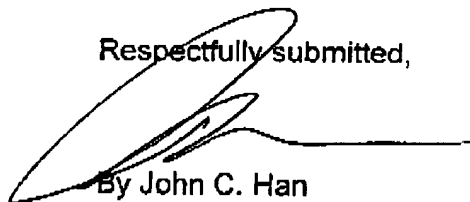
Appl. No. 09/692,709
Amdt. Dated July 14, 2004
Reply to Office action of April 15, 2004
Attorney Docket No. P12266/45687-00036
EUS/J/P/04-6160

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



By John C. Han
Registration No. 41,403

Date: July 14, 2004

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-7686
john.han@ericsson.com